2020

Cybercrime and Cyber security Techniques

Amy J. Ramson
CUNY Hostos Community College

Cyber Smart Yourself

An Introduction to Cybersecurity

Created For:

Hostos Community College

Created By:

eztechassist

Cyber Security & Managed IT Services

Presented By:

Shalom Cohen

This OER material was produced as a result of the CUNY Public Interest Technology initiative.

Creative Commons License

Created By:

eztechassist

Cyber Security & Managed IT Services

Presented By:

Shalom Cohen

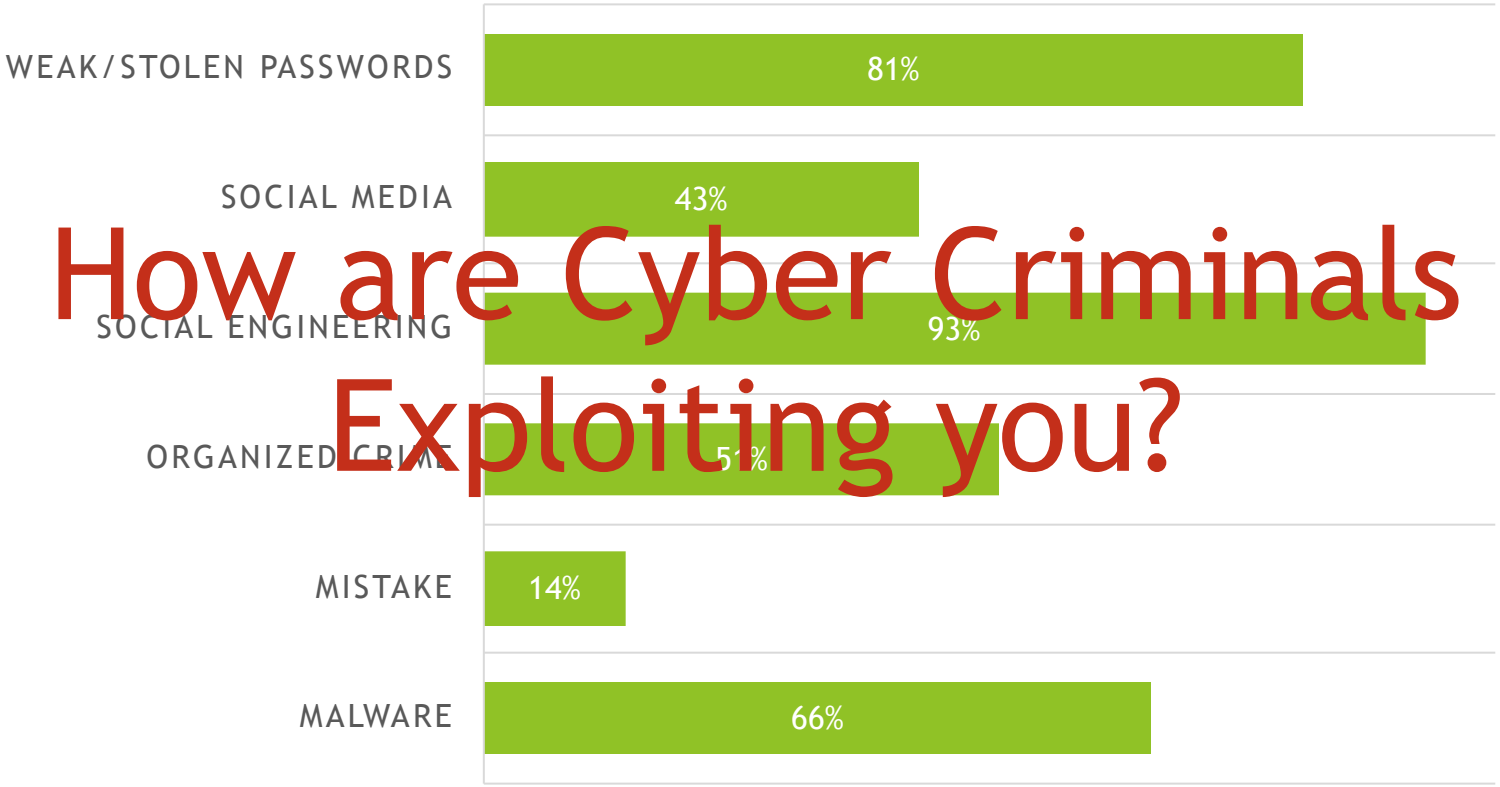
SCohen@eztechassist.com

95%

Cyber Crime can be avoided

Online Trust Alliance (OTA)

Cybersecurity Risk



How are Cyber Criminals Exploiting you?

eztechassist
Cyber Security & Managed IT Services

Cybersecurity & Me

Cybersecurity Myths

Understanding Exploits and Scams

Best Practices

Personal Identifiable Information

Laws & Regulation

Cybersecurity Myths

Why should I bother doing anything?

Hackers are not interested in me?

Are the apps in the Apple store and Google Play store safe?

Do I really need to keep so many passwords?

Are websites with the lock symbol safe to use?

Is a public WiFi secure if it requires a password?

Are email providers (Google & Yahoo) making money from my emails?

Cybersecurity Myths

Are my backups safe?

Do I need a separate email if I have a strong bank account password?

Will credit monitoring & Fraud alerts protect me?

Do I need to shred sensitive documents?

Can I be denied critically needed medicine at the hospital?

Understanding The Exploits

How do criminals get my money?

What do criminals do with my money?

How do criminals get my credentials?

What do criminals do with my credentials?

How do criminals access my computing resources?

What do criminals do with my computing resources?

Forms of Exploits

- Social Engineering
  - Phishing Attacks
    - Email Phishing
    - Spear Phishing
    - Whaling
    - Email account
    - Voice Phishing a.k.a. Vishing
    - SMS Phishing

Forms of Exploits

- Malware
  - Crypto mining & Cryptojacking
  - Ransomware
  - Spyware
  - Scareware
  - Adware
  - Trojans

Forms of Scams

Fake Technical Support

Government Agency Impersonation

Grandparent Scam

Virtual Kidnapping

Unpaid Utility Bill Scams

Online Dating Scams

Job Scams

Charity Scams

Robocalling Scams

Victim of a Phishing Attack

Disconnect from the Internet

Restart in Safe Mode

Backup your files

Change your account information

Fraud Alert & Freeze your credit

Victim of a Phishing Attack

Report the attack to authorities

- FBI – www.ic3.gov
- US-CERT – www.us-cert.gov
- FTC – www.ftccomplaintassistant.gov
- ISP – reportphishing@apwg.org
- Local Law Enforcement
- Identity Theft – www.identitytheft.gov

Victim of a Ransomware Attack

- Gather the evidence
- Disconnect from the Internet
- Screenshot of ransom note
- Decide to pay (negotiate) or not pay
- Restart in safe mode
- Identify the ransomware
  - www.nomoreransom.org/crypto-sherrif.php?lang=en
- Reinstall the operating system
- Report to Authorities

Protecting Your Money

Enable two-factor authentication

Create unique and complex passwords

Create a PIN

Maintain a separate email account

Dedicate a secure device

Bookmark your banking website

Use verified mobile apps

Enable security alerts

Use the “Chip” when available

Protecting Your Mobile Device

Use securely designed devices

Don’t use jailbroken devices

Enable lock screen code

Biometric risks

Encrypt your data

Apply updates

Backup to the cloud

Install verified apps

Protecting Your Mobile Device

Consider mobile A/V for Android

Enable ”Find My Device”

Beware of unsolicited texts & phone calls

Think before you click

Protecting Your Home WiFi

Use a modern WiFi Router

Lock down your WiFi router's console

Update your SSID name & Password

Update the firmware regularly

Apply strong encryption (WPA2)

Consider VPN services

Set up guest networks for visitors and IoT

Consider turning off your WiFi when not at home

Protecting Your IoT Devices

Review IoT Brands before purchasing

Review privacy policies

Change default password

Update the firmware regularly

Verify apps before downloading

Configure security and privacy settings

Set up a separate WiFi network for your IoT

Disable features you don’t need

Best Practices – Systems Security

- Keep antivirus software active and up-to-date
- Keep firewall software active and up-to-date
- Keep your operating system and programs up-to-date
- Regularly back up critical data
- Keep backed up data off-site
- Only download verified applications (PC & phone)
- Verify smart phone's apps access rights
- Don't click on links in texts from unknown senders

Best Practices – Email & Passwords

- Never open unknown attachments or links
- Use a secure document-sharing platform
- Guard login credentials to email and other services
- Use complex passwords
  - combination of letters, numbers, symbols
- Avoid using the same password for multiple accounts
- Consider using a password manager
- Use two-factor authentication whenever it is available
- Avoid doing business over unsecured networks
- Never mix work and personal information

What Needs to be Protected?

Most typical business, personal data and records are categorized into the following:

- Personally Identifiable Information (PII);
- Protected health information(PHI);
- Payments card data (PCI)

Personally Identifiable Information (PII);

- First and last name, a home or other physical address including street name and name of a city or town
- A screen or user name that functions as online contact information
- A telephone number
- A social security number
- A persistent identifier that can be used to recognize a user over time and across different websites or online services
- A photograph, video, or audio file, where such file contains an image or a voice
- Geolocation information sufficient to identify street name and name of a city or town; or
- the individual's past, present or future physical or mental health or condition
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual

Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act (FCRA) is the act that regulates the collection of credit information and the access to credit reports. It was passed in 1970 to ensure fairness, accuracy and privacy of the personal information contained in the files of the credit reporting agencies.

Under the FCRA, consumers have the right to:

Know what's in their file.

- Free file disclosure once per year from each of the major credit bureaus.
- Verify accuracy of report when required for employment purposes.
- Notification if a file has been used against them.
- Dispute and correct information that is incomplete or inaccurate.
- Remove outdated, negative information (seven years old or 10 years in the case of bankruptcy).

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA) is a law created to protect the privacy of children under 13. The Act was passed by the U.S. Congress in 1998 and took effect in April 2000. COPPA is managed by the Federal Trade Commission (FTC).

COPPA requires that site operators allow parents to review any information collected from their children. In practice, this means that any relevant site has to provide full access to all user records, profiles and log-in information when a parent requests it. The FTC has stipulated that parents may delete certain information but may not otherwise alter it.

Any Web site that collects information from children under the age of 13 has to abide by COPPA. The Act affects many popular sites like MySpace.com, Facebook.com, Friendster.com, Xanga.com and other social networking site

Section 5 FTC

Section 5 of the FTC Act, dating back to 1914, prohibits “unfair or deceptive business practices in or affecting commerce.” Not surprisingly for a law passed in 1914, the act does not mention cybersecurity. However, the FTC has long maintained that Congress intended for the word “unfair” to be interpreted broadly and flexibly to allow the agency to protect consumers as technology changes. Most early consumer privacy cases brought by the FTC came under the “deception” prong of Section 5. They targeted companies that gave false data security or privacy representations to their customers through websites or other applications.

Sarbanes-Oxley / SOX 404

Financial auditing of public companies

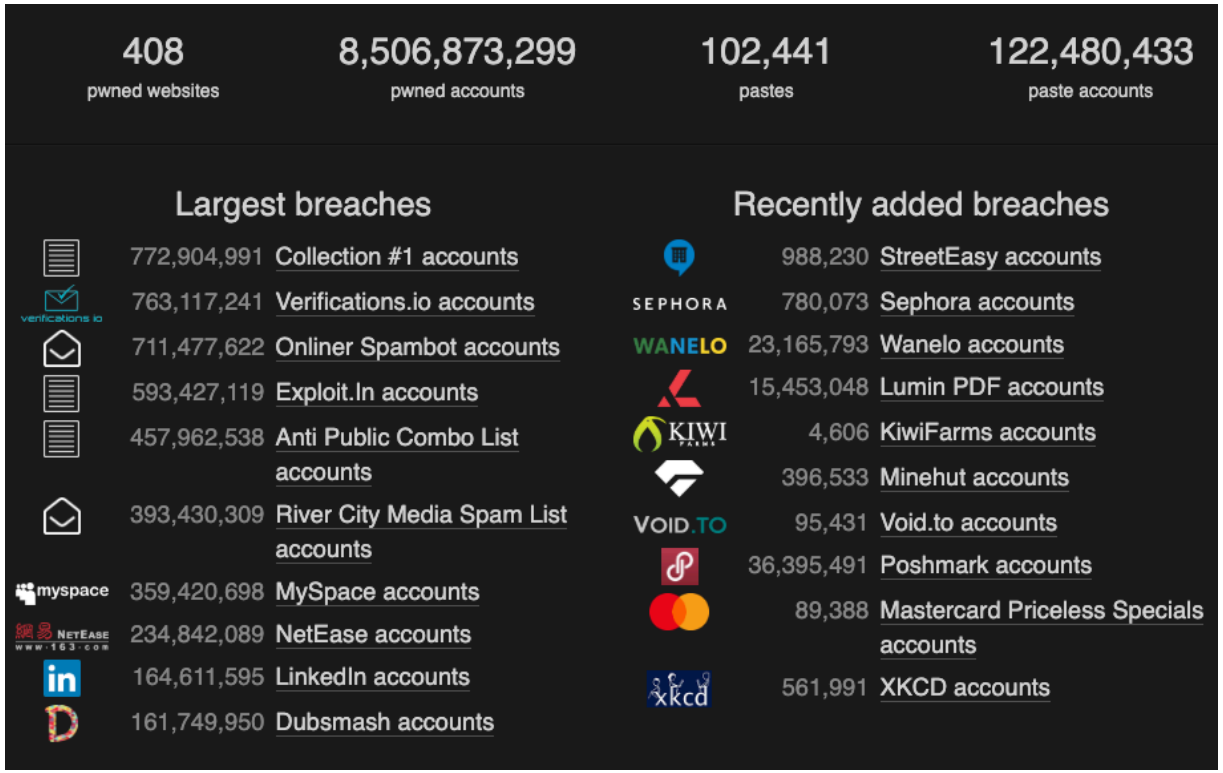
Includes auditing of security measures that affect financial reporting

Legislation has been introduced to apply to cybersecurity systems and cybersecurity systems officers the same requirements regarding corporate responsibility for financial reports and managements assessments of internal control structures and procedures for financial reporting as apply to public companies subject to oversight by the Securities and Exchange Commission (SEC)

Common Types of Personal Documents

- Bank Statements
- Paycheck Stubs
- Canceled checks
- Monthly and quarterly mutual fund and retirement contribution statements
- Credit Card Statements
- Medical Bills
- Utility Records
- Expired Insurance Policies
- Supporting Documents for Tax Returns
- Accident Reports and Claims
- Medical Bills
- Property Records and Improvement Receipts
- Sales Receipts
- Wage Garnishments
- Other Tax-Related Bills
- CPA Audit Reports
- Legal Records
- Important Correspondence
- Income Tax Returns
- Income Tax Payment Checks
- Investment Trade Confirmations
- Retirement and Pension Records
- Car Records
- Credit Card Receipts
- Insurance Policies
- Mortgages, Deeds Leases
- Pay Stubs
- Sales Receipts
- Stock and Bond Records
- Warranties and Instructions
- Other Bills
- Depreciation Schedules and Other Capital Asset Records

';--have I been pwned?



https://haveIbeenpwned.com

eztechassist
Cyber Security & Managed IT Services

So What's Next?

Open Source Security Tools

Nmap

Nmap - map your network and ports with the number one port scanning tool. Nmap now features powerful NSE scripts that can detect vulnerabilities, misconfiguration and security related information around network services.

Scan a single IP	`nmap 192.168.1.1`
Scan a host	`nmap www.testhostname.com`
Scan a range of IPs	`nmap 192.168.1.1-20`
Scan a subnet	`nmap 192.168.1.0/24`
Scan targets from a text file	`nmap -iL list-of-ips.txt`

OpenVAS

OpenVAS - open source vulnerability scanning suite that grew from a fork of the Nessus engine when it went commercial. Manage all aspects of a security vulnerability management system from web based dashboards.

The primary reason to use this scan type is to perform comprehensive security testing of an IP address. It will initially perform a port scan of an IP address to find open services. Once listening services are discovered they are then tested for known vulnerabilities and mis-configuration using a large database (more than 53000 NVT checks). The results are then compiled into a report with detailed information regarding each vulnerability and notable issues discovered.

WireShark

Wireshark - view traffic in as much detail as you want. Use Wireshark to follow network streams and find problems. Tcpdump and Tshark are command line alternatives. Wireshark runs on Windows, Linux, FreeBSD or OSX based systems.

- Detect anomalous behaviour that could indicate malware
- Search for unusual domains or IP address endpoints
- Use IO graphs to discover regular connections (beacons) to command and control servers
- Filter out the "normal" and find the unusual
- Extract large DNS responses and other oddness which may indicate malware

WireShark.org

Kali Linux

Kali Linux - was built from the foundation of BackTrack Linux. Kali is a security testing Linux distribution based on Debian. It comes prepackaged with hundreds of powerful security testing tools. From Airodump-ng with wireless injection drivers to Metasploit this bundle saves security testers a great deal of time configuring tools.

Kali.org

Shodan

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

shodan.io

eztechassist

Cyber Security & Managed IT Services

(888) 859-2688

support@eztechassist.com